PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-296076
(43)Date of publication of application : 29.10.1999

(51)Int.Cl. G09C 1/00
G09C 1/00

(21)Application number : 10-073656
(22)Date of filing : 23.03.1998

(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>
(72)Inventor : KUDO MICHIHARU

(54) METHOD AND SYSTEM FOR SMALL TIME KEY GENERATION

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain a method and system for generating a small time key from a time key.
SOLUTION: Plural small time keys are generated within a time unit. A unit time deciphering key right after the time unit is generated (710). A unidirectional function is applied to the unit time deciphering key to obtain a final small time key (720). A small time key to be found is obtained by applying the unidirectional function to the small time key right before the small time key to be found. Namely, the small time key is generated from the small time key in the final order forward in time series (730). Consequently, even if a specific small time key leaks out for some reason, it is impossible to generate a small time key which is precedent in time series on the basis of the specific small time key. Further, the unit time deciphering key is safe even when small time keys are made open one after another.